

Resources

FirstGov for Consumers
www.consumer.gov

Internet Fraud Complaint Center
www.ifccfbi.gov

Federal Trade Commission
www.ftc.gov

Federal Bureau of Investigation
www.fbi.gov

Securities and Exchange Commission
www.sec.gov

U.S. Postal Inspection Service
www.usps.com

U.S. Department of Justice
www.internetfraud.usdoj.gov

National Association of Attorneys General
www.naag.org

American Association of Retired Persons
www.aarp.org

Better Business Bureau
www.bbb.org or www.bbbonline.org

Internet Fraud Council
www.internetfraudcouncil.net

National Fraud Information Center
www.fraud.org

About the Cybercrime Task Force

The Utah Cybercrime Task Force (UCTF) is a partnership between federal, state, and local law enforcement agencies. The task force is led by the Utah Attorney General's Office. Partners include the Federal Bureau of Investigation, the U.S. Department of Defense, and the Salt Lake City Police Department.

The task force handles crimes committed via computer systems, including

- Internet Fraud
- Identity Theft
- Computer Intrusion
- Computer or Internet-related Extortion
- Cyberstalking
- Other Computer-oriented Crime*

*Internet crimes related to child pornography and child abuse are handled by the Utah Internet Crimes Against Children Taskforce. You can contact them at (801) 596-0907 or go to www.utahicac.com for more information.

For more information about the
task force, please send an email to
cybercrime@utah.gov
or go to
www.attorneygeneral.utah.gov



Utah Attorney General's Office

Don't Become a Victim of Computer Fraud



(801) 366-0260 or 800-244-4636
5272 S. College Drive, #200
Murray, UT 84123

Common Scams

Nigerian Money Offers

Someone contacts you from Nigeria or another African country and offers you millions of dollars. You're told all you have to do is help transfer money, diamonds or other riches to your bank account for safekeeping. These promises are not true. They really want to take money from your account, not put money into it.

Auction Fraud

You participate in an online auction and win the bid for the item. You pay for the item but never receive it.

Job Offers

You apply for a job online. You are hired and now must provide to your new "employer" your personal information and bank account information. You never really had a new job, but now someone has your identity to use fraudulently and your bank account information to take your money.

Unsolicited Email

You receive an email asking for personal or financial information. Your information is used to steal your identity or access your financial accounts.

How to Protect Yourself

Do some research. Check with other agencies to validate the legitimacy of the company making the offer or asking for information (see "Resources" section). Call or write to the company to validate the offer.

Educate yourself. Learn about the different online fraud scams (see Resources section).

Don't judge by initial appearances. Remember, just because something appears on the internet doesn't mean it's true.

Pay by credit card or escrow service. Make sure the credit card company you are using has a fraud protection policy. Review your credit card statements each month for unauthorized transactions. Beware of phony escrow services.

Be cautious of online sellers who want you to send checks or money orders immediately to a post office box before you receive the goods or services you've been promised.

Watch out for fraudulent positive "feedback" of sellers.

Don't provide personal information (social security number, birthdate, passwords, etc.) or financial information (bank account numbers, credit card numbers, etc.) to anyone you don't know or who is soliciting information from you.

What to Do If You Are a Victim

File a report with your local police department. Make note of your case number. You may need it later.

Contact any financial institutions involved in the fraudulent transaction, such as banks, credit card companies, etc.

Keep record of all contacts you make and follow up with them in writing.

If the transaction could affect your credit, contact one of the three major credit reporting bureaus:

| | |
|-------------|----------------|
| Experian: | 1-888-397-3742 |
| Equifax: | 1-800-525-6285 |
| TransUnion: | 1-800-680-7289 |

File a complaint with the Internet Fraud Complaint Center at www.ifccfbi.gov